REMARKS

Claims 1-24 are pending in the application. Claims 1-20 have been examined and stand rejected. Claims 1, 11-13, 16, 19 and 20 have been amended, and new claims 21-24 have been added. It is noted that the amendments to at least independent claims 1, 11 and 19 only include slight amendments that should not significantly change the scope of the claims. The remaining claim amendments are supported by the specification and drawings. Favorable reconsideration of the application and allowance of all of the pending claims are respectfully requested in view of the following remarks.

The Examiner objects to the specification, alleging that it contains an embedded hyperlink and/or other form of browser-executable code. The Examiner requires deletion of this text. This objection is respectfully traversed. It is noted that page 6, lines 5-9, of the specification lists two website domain name addresses to which specifications describing two example protocols for encrypting/decrypting content are located (i.e., HDCP revision 1.1, which can be downloaded at the website address www.digital-cp.com, and DCTP specification version 1.3, which can be downloaded at the website address www.dtcp.com). It is respectfully submitted that these two website domain name addresses are not hyperlinks within the specification but merely provide information regarding a publication source from which one can locate the cited specifications (i.e., analogous to a journal reference for other forms of non-patent literature documents). The Examiner is therefore requested to reconsider and withdraw this objection to the specification.

The Examiner objects to claims 12 and 13 for certain informalities, and corrections to these claims have been made by amendment to address these informalities. The Examiner is therefore requested to reconsider and withdraw the objections to these claims.

Claims 2, 3, 12 and 13 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite since these claims recite the use of protocols for high-width digital content protection or digital transmission content protection. The Examiner alleges that it is unclear exactly what

protocols would be recognized in the art as being for these specific purposes. This rejection is respectfully traversed.

The specification (at page 5, line 29 to page 6, line 9) clearly and sufficiently sets forth that an authority such as a consortium of digital content providers or a consortium of manufacturers provides device key sets to "authorized" manufacturers of digital subscriber services, where the consortium establishes protocols by which "shared secrets" are determined between settop terminals and subscriber devices and for encrypting/decrypting of content. In addition, non-limiting examples of such protocols are provided in the specification (HDCP, DTCP, and OpenCable CableCARD Copy Protection System). Further, the specification provides two specific examples of such protocols (HDCP revision 1.1. and DCTP specification version 1.3).

When considering claims 2, 3, 12 and 13 in view of the disclosure in the specification regarding protocols associated with HDCP and DTCP, these claims are clear and definite and one having ordinary skill in the art would clearly understand and recognize what is being referred to in relation to the use of protocols as recited in these claims. The Examiner is therefore requested to reconsider and withdraw the rejections of claims 2, 3, 12 and 13 under 35 U.S.C. §112, second paragraph.

Claims 1-3, 6, 10-13 and 16 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,937,067 to Thatcher et al. ("Thatcher"); claims 4, 5, 14 and 15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Thatcher; claims 7-9 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Thatcher in view of U.S. Patent No. 6,157,719 to Wasilewski et al. ("Wasilewski"); and claims 17-20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Thatcher in view of Komuro et al. ("Komuro"). These claim rejections are respectfully traversed.

The present invention relates to transmission of protected digital content from a settop terminal to a subscriber device in communication with the settop terminal. In an example embodiment (shown in Figs. 2-5 of the application), a digital subscriber communication terminal

or DCST includes a memory 206 in which is stored an encrypted device key set (EDKS) 228 and an encrypted device key set decryptor (EDKSD) 230 and a separate, secure element 208 that includes a processor 302 and a memory 304 in which is stored a number of items including a message private key (MPK) 314 and a key decryptor private key (KDPK) 316. The KDPK 316 is a private key of a private key/public key pair, and this private key is only accessible by processor 302. The DCST further includes an adaptive output interface (AOI) 220 that is in two-way communication with a subscriber device 108 (e.g., a television) via a communication link 224 that supports outputting content according to standards such as, but not limited to, DVI, DTCP and HDCP (e.g., a DVI interface or an IEEE 1394 interface).

The present invention prevents unauthorized copying or use of digital content (which is received by the DCST from a headend) using the KDPK 316, EDKSD 230, and EDKS 228, which are used to generate a device key set (DKS) 226 and send the DKS 226 to the AOI 220. In operation, a DKS 226 is generated by first passing EDKSD 230 from memory 206 to secure element 208, where EDKSD 230 is decrypted by KDPK 316 using processor 302 within secure element 208 so as to generate a device key set decryptor (DKSD). The DKSD is then passed from secure element 208 to processor 204, which decrypts EKDS 228 using the DKSD to generate DKS 226. The DKS 226 is then passed to AOI 220. The AOI 220 detects the presence of a subscriber device 106, via communication link 224, and uses DKS 226 to determine whether the subscriber device 106 is authorized to received digital content from the DCST.

As noted in the specification (page 5, line 29, to page 6,line 9), an authorized subscriber device will include a device key set which is typically provided to the device during its manufacture, where an authority such as a consortium of digital content providers or manufacturers provides such device key sets to authorized digital subscriber devices. The AOI 220 communicates with the subscriber device 108, using the DKS 226, to determine whether device 108 is authorized to receive digital content from the DCST. If the device 108 is determined as authorized to receive digital content, the AOI 220 uses a "shared secret" with the device 108 to encrypt digital content and transmit the encrypted digital content to the device 108

via communication link 224. The subscriber device is capable of decrypting the encrypted digital content only if the "shared secret" has been determined using the DKS 226. The AOI 220 can inhibit transmission of protected content to subscriber device 108 if no "shared secret" has been determined.

Therefore, the present invention relates to a method of protecting digital content that the settop terminal has already received and processed from a headend, where the settop terminal transfers protected digital content in a manner available for use or display to a subscriber device only if and when the settop terminal has confirmed the subscriber device is authorized to receive such protected digital content.

The previously described decryptor keys and device key set are not used to decrypt entitlement management messages (EMMs) or entitlement control messages (ECMs) sent from the headend to the settop terminal. Rather, as noted in the specification (page 7, lines 24-33), the message private key (MPK) 314 stored within secure element 208 decrypts EMMs sent to the DSCT by the headend.

Each of the claims recites a settop terminal or a method that is implemented within a settop terminal. In particular, claim 1 recites a settop terminal in a subscriber television system, the settop terminal comprising a first memory including an encrypted first key and an encrypted device key set stored therein, a secure element including a processor and a second memory, where the second memory is accessible only to the processor and has a private-key of a private-key/public-key pair stored therein, where the processor is adapted to decrypt the encrypted first key using the private-key, and where the decrypted first key is used to decrypt the encrypted device key set, and an adaptive output interface adapted to utilize a device key set to determine a shared-secret key with a receiver in communication therewith and adapted to provide an encrypted stream of content to the receiver using the shared-secret key to encrypt the stream of content.

Claim 11 recites, in a subscriber television system including a headend in communication with a plurality of settop terminals including a given settop terminal, the given settop terminal

comprising a first memory including an encrypted first key and an encrypted device key set stored therein, a secure element including a first processor and a second memory, where the second memory is accessible only to the first processor and has a private-key of a private-key/public-key pair stored therein, where the first processor is adapted to decrypt the encrypted first key using the private-key, an input port receiving a stream of content from the headend, a second processor adapted to determine from the stream of content whether the content of the stream of content is protected and adapted to receive the decrypted first key and decrypt the encrypted device key set using the decrypted first key, and an adaptive output interface adapted to implement the decrypted device key set to determine a shared-secret key with a receiver in communication therewith and, responsive to the first processor determining the content is protected, adapted to provide an encrypted stream of content to the receiver using the shared-secret key to encrypt the stream of content, and, responsive to the first processor determining the content is not protected, adapted to provide the stream of content to the receiver.

Claim 16 recites a method of providing a receiver with a stream of content, the method implemented in a settop terminal in a subscriber television system, the method comprising the steps of decrypting an encrypted first key using a private-key of a private-key/public-key pair belonging to the settop terminal, wherein the first key is decrypted inside of a secure-element including a processor and a memory, wherein the private-key is accessible to only the processor, decrypting an encrypted device key set using the decrypted first key, providing the decrypted device key set to an adaptive output interface of the settop terminal that is in communication with the receiver, determining a shared-secret key with the receiver using the decrypted device key set, and outputting the stream of content to the receiver.

Claim 19 recites a method of providing a receiver with a stream of content, the method implemented in a settop terminal in a subscriber television system, the method comprising the steps of decrypting an encrypted first key using a private-key of a private-key/public-key pair belonging to the settop terminal, where the first key is decrypted inside of a secure-element including a processor and a memory, where the memory is accessible to only the processor and

has the private-key stored therein, decrypting an encrypted device key set using the decrypted first key, providing the decrypted device key set to an adaptive output interface, negotiating a shared-secret key with the receiver using the decrypted device key set, receiving a stream of content from a headend of the subscriber television system, determining whether the receiver is entitled to access the stream of content, determining whether the received stream of content is encrypted content, and outputting the stream of content to the receiver.

Thatcher fails to teach or suggest the combination of features of each of claims 1, 11, 16 and 19.

Thatcher describes a system and corresponding method for local encryption of a global transport data stream (TDS), where local cable head end operators can locally control access to individual subscriber decoders independent from a nationally provided TDS. As noted by Thatcher (see Col. 4, lines 38-61), entitlement management messages (EMMs) and entitlement control messages (ECMs) are multiplexed into the TDS, where ECMs are broadcast to all decoders and include seed data encrypted under a multi-session key (MSK). The MSK is encrypted under a secret serial number (SSN) and is included in the EMM, and the EMM is addressed to a decoder that has stored in it the SSN that was used to encrypt the MSK. The seed data includes seeds that are used by the decoder to decrypt authorized services for the subscriber associated with this decoder (as identified by its SSN).

In rejecting the claims, it is unclear whether the Examiner has interpreted the claimed subject matter to read upon an encryption control system provided by the local headend operator (as shown in the embodiments of Figs. 6, 7 and 8 of Thatcher), a decoder that receives a TDS (as shown in Fig. 5 of Thatcher), or combinations of the encryption control system and decoder. Each one of these possibilities is addressed below.

The decoder described in Fig. 5 of Thatcher would most likely be disposed within a settop terminal and therefore appears to be most relevant to the claims (which, as noted above, recite a settop terminal or methods implemented within a settop terminal). The decoder 80 includes a secure memory 82 that stores a secret serial number SSN and a multi-session key

MSK. A demultiplexer 72 receives the TDS and separates the EMM 76 from text data 78 and sends the EMM 76 to a decryptor 84. The decryptor 84 processes EMM, using SSN, to recover MSK and stores MSK in memory 82. The MSK is then provided to another decryptor 86 that receives and processes ECM 74 to recover seeds and other conditional access data 88. The seeds and other conditional access data 88 are sent to conditional access logic 90, which processes this data to identify authorized services and provides a service selection signal 96 to service to demultiplexer 106 and encrypted service seeds 98 to decryptor 100 for decryption by the MSK. The decryptor 100 provides seeds 102 to decryptors 108 for authorized services.

From the Examiner's rejection, it appears that the Examiner construes the SSN of Thatcher with the private-key of a private-key/public-key pair stored in a memory of the secure element as recited in the claims. This would mean that the encrypted MSK, which is decrypted using the SSN, would be construed by the Examiner as the recited encrypted first key (since the claims recite that the private-key decrypts the encrypted first key).

It is noted that claims 1 and 11 recite that the encrypted first key is stored within a first memory and the private-key of a private-key/public key pair is stored in a second memory within the secure element. As described and shown in Fig. 5 of Thatcher, a single memory 82 stores both the MSK and the SSN. Therefore, Thatcher cannot anticipate claims 1 and 11 for at least this reason.

Thatcher further describes that the MSK, after being decrypted by the SSN, is used to decrypt seeds that are provided to the decoder within the ECM 74. This would mean that the Examiner construes the decrypted seeds as the recited device key set that is decrypted by the decrypted first key (construed by the Examiner as the MSK).

Based upon such an interpretation of the decoder of Fig. 5 of Thatcher, there is no disclosure or suggestion whatsoever of an adaptive output interface as recited in the claims, where the adaptive output interface (AOI) utilizes the device key set (apparently construed by the Examiner as the decrypted seeds) to determine a shared-secret key with a receiver in communication with the AOI and to provide an encrypted stream of content to the receiver using

the shared-secret key to encrypt the stream of content. Rather, the decrypted services 109 shown in Fig. 5 of Thatcher, which are determined based upon the seeds which have been decrypted by the MSK, appear to be provided to a receiver in communication with decoder 70 without any type of determination of a shared-secret using a device key set provided to an AOI as recited in each of claims 1, 11, 16 and 19.

Therefore, the embodiment of Fig. 5 fails of Thatcher fails to anticipate or render obvious each of claims 1, 11, 16 and 19.

In the embodiment of Figs. 6-8 of Thatcher, embodiments of the local headend operator are shown, where the local headend operator receives the national TDS from a national source and decrypts the MSK from the national EMM and/or seeds from the national ECM followed by encryption of the MSK into a local EMM and/or seeds into a local ECM for transfer within a local TDS to be sent to subscriber decoders of the local headend operator. For example, in Fig. 6 of Thatcher, the encryption control system 110 of the local headend operator decrypts the MSK in national TDS using a SSN 122, and then encrypts the MSK using SSN stored in memory 132 within a local EMM to be provided in local TDS with national ECM to subscriber decoders, where the subscriber decoders have SSNs which correspond with SSN stored within memory 132. As noted by Thatcher, this allows the local head-end operator to deny access for national services to a subscriber when, for example, the subscriber fails to pay its bill (see Col. 6, lines 18-38 of Thatcher).

The embodiments of Figs. 7 and 8 of Thatcher show other variations for the encryption control system of the local headend operator. In particular, in the embodiment of Fig. 7, the seeds of the national ECM are decrypted using MSK and SSN in memory 122 and then encrypted using MSK and SSN in memory 122 to generate a local ECM that is provided with the national EMM in a local TDS. In the embodiment of Fig. 8, the encryption system 150 of the local headend recovers an unencrypted frame of service data using a global seed and then re-encrypts the service data using a new seed provided by a seed generator 152. The encryption system 150 further generates a local ECM with an MSK encrypted with encryptor 144. A unique

encryption algorithm can be used in system 150 that corresponds with a respective decrypted algorithm in subscriber decoders for the local headend.

In each of the embodiments of Figs. 6-8, the SSN of Thatcher might be construed as the private-key of a private-key/public key pair as recited in the claims, which would lead to the encrypted MSK of Thatcher being construed as the encrypted first key as recited in the claims (since the SSN is used to decrypt the encrypted MSK within national EMM). As noted above, the MSK of Thatcher is used to decrypt seeds within the ECM, whether it is the national ECM or a local ECM generated by the encryption system of the local headend. Therefore, this would lead to the seeds being construed as the device key set as recited in the claims.

There is no teaching or suggestion whatsoever in the Figs. 6-8 embodiments of Thatcher of any AOI as recited in the claims, where a device key set provided to the AOI is used to determine a shared-secret key with a receiver in communication therewith to provide an encrypted stream of content to the receiver using the shared-secret key to encrypt the stream of content. The seeds which are encrypted and provided in the national ECM or local ECM of Thatcher are not used as a device key set to determine a shared-secret key.

At best, the SSN described in Thatcher, and not the seeds, might be construed as a key that is shared between the local headend and the subscriber decoders, since it is the common or corresponding SSNs that facilitate decrypting of MSKs in EMMs which in turn facilitate decrypting of seeds in ECMs provided to the subscriber decoders. However, assuming the SSN is to be construed by the Examiner as the recited device key set and/or shared-secret key feature of the claims, then there is no teaching or suggestion of the recited private-key and encrypted first key features as recited in the independent claims.

Therefore, none of the embodiments of Figs. 6-8 of Thatcher, when considered alone or together, teaches or suggests the combination of features of each of claims 1, 11, 16 and 19.

In addition, it would be improper to attempt to construe elements from the combination of the decoder described in Fig. 5 of Thatcher with the encryption control system shown in any of Figs. 6-8 of Thatcher, since the claims recite a settop terminal or a method in which all

method steps are implemented within the settop terminal (i.e., within a single device). The decoder of Fig. 5 appears to be in relation to a settop terminal and is a separate device from the local headend encryption systems described in Figs. 6-8.

For all the foregoing reasons, it is respectfully submitted that Thatcher fails to anticipate or render obvious the combination of features of each of claims 1, 11, 16 and 19. The Examiner is therefore requested to reconsider and withdraw the rejections of claims 1, 11 and 16 as being anticipated by Thatcher.

In addition, each of Wasilewski and Komuro fails to make up for the above-noted deficiencies of Thatcher with respect to claim 19.

Therefore, claim 19 is not obvious over any combination of Thatcher with Komuro, and the Examiner is requested to reconsider and withdraw the rejection of claim 19 based upon this combination of references.

Claims 2-10, 12-15, 17, 18 and 20 depend from one of claims 1, 11, 16 and 19 and therefore include all of the features of their respective parent claims. The Examiner is therefore requested to reconsider and withdraw the rejection of these claims based upon Thatcher or Thatcher in combination with Wasilewski or Komuro.

New claims 21-24 depend from one of the independent claims and should therefore also be allowed for at least the reasons noted above with respect to their parent claims. In addition, each of these new claims includes additional features which are not taught or suggested by Thatcher or any combination of Thatcher with Wasilewski or Komuro.

In particular, claims 21 and 22 further recite that the memory of the secure element further includes a message private key stored therein that is separate from the private-key, where the processor of the secure element is further adapted to decrypt data within entitlement management messages (EMM) provided by the headend of the subscriber television system to the settop terminal using the message private key. Claims 23 and 24 further recite the features of providing an entitlement management message (EMM) from a headend of the subscriber television system to the settop terminal, and decrypting data within the entitlement management

message (EMM) with a message private key stored within the memory of the secure-element, where the message private key is separate from the private-key.

Since the SSN of Thatcher is clearly used to decrypt data within the EMM (i.e., the MSK), the SSN cannot reasonably be construed as the private-key of claims 21-24, since these claims recite the further feature of a message private key that is separate from the private-key and that is used to decrypt data within the EMM.

In view of the foregoing, Applicants respectfully request the Examiner to find claims 1-24 to be in condition for allowance. However, if for any reason the Examiner feels that the application is not now in condition for allowance, the Examiner is respectfully requested to call the undersigned attorney to discuss any unresolved issues and to expedite the disposition of the application.

Applicants hereby petition for any extension of time that may be necessary to maintain the pendency of this application. An excess claim fee for 4 additional claims over 20 is also being paid electronically with submission of this paper. In addition, the Commissioner is hereby authorized to charge payment of any additional fees required for the above-identified application or credit any overpayment to Deposit Account No. 05-0460.

Dated: September 22, 2008

Respectfully submitted by:

/Andrew J. Aldag/

Andrew J. Aldag
Reg. No. 40483

EDELL, SHAPIRO & FINNAN, LLC
CUSTOMER NO. 05642
1901 Research Boulevard, Suite 400
Rockville, MD 20850
(301) 424-3640